1ID PAM 1-201
COMMAND INSPECTION CHECKLIST

FUNCTIONAL AREA: G6 – AMO	CHAPTER: 16 SECTION: B	DATE OF REVISION: 1 MAY 03
PROPONENT/PHONE NO: G6 Automation 350-6386/6387	PROGRAM/ACTIVITY/TOPIC (PAT) Information Assurance	UNIT INSPECTED/DATE:

ITEM	GO	NO-GO
A. Discussion: 1. This inspection applies to brigades, battalions, battalion separates, and company separates. Information Systems Security is a composite of means to protect telecommunications and automated information systems and the information they process. These means include primarily physical security, automated information systems security, and communications security. 2. The purpose of Information System Security is to protect all sensitive defense information processed by Automated Information System (AIS) resources, regardless of application, functional proponent, or source of funding. Automated information Security is the safeguarding of automation equipment and information against unauthorized access, modification, use, destruction or denial of use, theft, and sabotage. 3. The purpose of the Information Systems Security inspection is to ensure that the Commanding General's guidance and appropriate regulatory automation are being adhered to. The inspection consists of the following areas: Information Security, Software Controls, and Password/Access Controls as rightly pertain to computers (servers, PCs, and laptops), battlefield automation systems (e.g., ULLS, TACCS, MCS, MSE) and fax equipment. B. References: 1. AR 190-13, 30 SEP 93, The Army Physical Security Program. 2. AR 380-5, 25 FEB 88, and USAREUR Suppl 1, 18 JUL 89, Department of the Army Information Security Program. 3. AR 380-19, 27 FEB 98, Information Systems Security. 4. AR 380-67, 9 SEP 88, and USAREUR Suppl 1, 20 JAN 94, Personnel Security Program. 5. AR 710-2, 31 OCT 97, Supply Policy Below the Wholesale Level, (Unit Supply Update). 6. USAREUR Regulation 380-19, 28 MAY 91, Information Systems Security. 7. 1ID Pamphlet 25-1, 1 APR 96, Automation Management. 8. Message: DA WASHINGTON DC/SAIS-IAS// 281818Z JUN 00. 9. USAREUR Command Policy Letter 4, Information Assurance 6 November 2001. C. Specific Questions: **Duty Appointments** *1. Has each Subordinate Command, separate battalion, and separate company appointed an Information Assurance Officer (IAO) on orders to establish and implement the Information Systems Security program within the command or unit? Has a copy of the appointment orders been provided to the Division IAM? (para 1-6d (2), AR 380-19 and para 4d (3), 4d (6), 4(g), UR 380-19), and DA Message 281818Z JUN 00.		

ITEM	GO	NO-GO
Accreditation – Documentation and Program Requirements		
∗2. Are all information systems and networks accredited and certified?		
∗3. Have all personnel received the level of training necessary and appropriate to perform their designated information assurance responsibilities?		
*4. Has the unit established a risk management program for each automated system? (para 1-6d (2)f, 1-6d (3) (c), 1-6d (4) (e) and Chapter 5, AR 380-19)		
*5. Has a periodic review of the risk management program taken place in the recent past?		
∗6. Are the appropriate leadership/management personnel aware of the results of risk Analysis/vulnerability assessments?		
7. Does a risk management plan address risks of damage, espionage, sabotage, and theft to each system? (para 5-1a, AR 380-19 and para 33, UR 380-19)		
∗8. Are countermeasures identified based on the results of risk analysis/vulnerability assessments?		
∗9. Are countermeasures reasonable in terms of practicality, time, cost and security? (para 5-4b, AR 380-19)		
∗10. Is there a written security plan to document implementation of countermeasures?		
∗11. Are countermeasures routinely tested (for example, user IDs, passwords, audit trails)?		
∗12. Is there a Continuity of Operations Plan? (Required for mission essential systems within USAREUR) (para 31, UR 380-19)		
13. Has the Designated Accreditation Authority of those systems used to transmit Sensitive But Unclassified level information been granted a waiver in lieu of using an approved NSA encryption device? NOTE: This requirement applies to FAX equipment as well as computer systems. (para 1-6d(2) (d) and (e), 2-2 2-3a(10), 3-sd and 3-6, AR 380-19, para 36, UR 380-19)		
14. Has each AIS been assigned a sensitivity level, security processing mode and been properly accredited prior to operation? Has the unit conducted its reaccreditation of computer systems when any changes to the system have occurred? (para 1-6d (2) (d) and (e), 2-2, 2-3a (1), 3-sd and 3-6, AR 380-19, para 36, UR 380-19)		
15. Has the unit applied as a minimum, the FOUO marking to the accreditation document? (para 3-sc, AR 380-19 and para 37f (1), UR 380-19)		
16. Has the unit forwarded their request for accreditation to the appropriate authority in sufficient time to be acted upon before operation of the system or the expiration of any existing accreditation. (para 3-sd, AR 380-19)		
17. Does the IAM/IAO provide assistance and review accreditation to the appropriate accreditation authority for signature? (para 1-6d (3) (h), AR 380-19, para 4h(6) and 34c, UR 380-19		
18. Does the IAO maintain an inventory of all assigned and tenant unit automated systems to include their accreditation status? (para 3-7, AR 380-19)		
19. Are copies of all accreditation and reaccredidation records maintained on file by the appointed IAO? (para 41a(1), UR 380-19)		
20. Has the unit conducted its accreditation review? (para 3-1b (4), AR 380-19)		

ITEM	GO	NO-GO
AIS Operations		
21. Has the appointed IAO developed an SOP for use within the unit that outlines the security of system operations? (para 1-6d (3) (b) AR 380-19)		
22. Does the unit have an access control policy for each AIS? (para 2-3a (2), AR 380-19)		
*23. Is classified magnetic media safeguarded in accordance with the highest classification for which it was used? (para 2-19b, AR 380-19)		
24. Does the security plan for tactical or battlefield automation systems (BAS) and office systems used in the filed include measures to enhance security during transportation mechanisms available to render BAS or office systems in the filed inoperable in case of imminent capture, and methods of destroying classified information both in hard copy and on AIS media? (para 2-26d, AR 380-19)		
*25. Are all personnel who manage or access AIS resources provided an appropriate security briefing prior to beginning their assigned duties and annually thereafter? (para 2-16, AR 380-19 and para 16a, UR 380-19)		
26. Are only personnel with appropriate clearance levels and the need to know allowed access to the system/diskette which are used to process classified or unclassified sensitive information and is classified magnetic media declassified and/or destroyed when no longer required? (para 7-100a, 7-105 and 9-100, AR 380-5, and para 2-19b and AR 380-19)		
27. In systems containing NONREMOVABLE magnetic media for processing of classified information, does the system meet the security requirements of non-removable storage media? If not, has the designated Automated Accreditation Authority authorized its use, and are countermeasures implemented to ensure that classified information is not written to the system's hard disk? (para 2-22 and 2-27c, AR 380-19)		
28. If removable magnetic media is used for the storage of classified information, has it been externally marked with the appropriate SF label? Are classified documents internally portion marked with the appropriate classification? (para 4-304 and 4-305, AR 380-5, para 2-20, AR 380-19)		
29. Are printer ribbons controlled and marked according to their classification and destroyed as classified material? (para 5-201c, AR 380-5)		
30. Has an SF Form 701, (Activity Security Checklist) been posted within those areas used for classified material? (para 5-202, AR 380-5)		
31. If removable magnetic media is used for the storage of classified information, has it been marked with the appropriate classification?		
32. Has the appropriate SF label been affixed to the removable media? (para 4-304, AR 380-5 and AR 380-19)		
33. Are classified documents' internal portions marked with the appropriate classification? (para 4-304 and 4-305, AR 380-5, and para 2-20, AR 380-19)		
34. Is classified magnetic media maintained as classified material and declassified or destroyed when no longer needed? (para 4-303, 4-304, 9-100, and para k-5f, Appendix K, AR 380-s, and para 2-3a(5) and 2-21, AR 380-19)		

ITEM	GO	NO-GO
Report Requirements		
*35. Is a list, kept by the IAO, of signatures and dates briefed for all personnel who receive the briefing available for review? (para 2-16, AR 380-19, and 16a and D-4, UR 380-19)		
*36. Does the IAO report all serious or potentially serious security violations involving automation activities, including virus infections/attacks through information security channels to the Commander, 1st Infantry Division, ATTN: AETV-BGB-CI (para 1-6d (2), 1-6d (3) (g), 2-28, para 7 and Appendix F UR 380-19)		
Software Controls		
37. Is only software that has been procured through an authorized contractor representative been authorized for use on a government AIS? (para 2-4b, AR 380-19)		
38. Does the unit have public domain, shareware or privately owned software? If so has it been approved by the Division IAM? (para 2-4b, AR 380-19 and para 8 and 29, UR 380-19)		
39. Does each AIS have an approved listing of software that is authorized to be run on that AIS and are the original diskettes and manuals available? Is the software application removed from systems for which original software is not available? (para 2-4d, AR 380-19)		
40. Has the unit IAO established a system for issuing, protecting, and changing system passwords? (para 1-6d(3) (j), AR 380-19)		
41. Are persons having access to passwords instructed on the sensitivity and protection of such passwords? (par 2-25g, AR 380-19)		
42. If passwords are used have they been randomly generated? (para 2-15d and 2-15k, AR 380-19)		
43. Does the IAO maintain a list of personnel with password access, and when personnel no longer require access or have departed, are these personnel removed from access and their passwords retired? (para 2-15h, AE 380-19 and para 19, UR 380-19)		
44. Are the passwords changed at least four times a year for AIS used to process classified information? (para 2-14g, AR 380-19)		
45. Are passwords for other AIS changed at least twice every year? (para 2-14g, AR 380-19)		
*46. Are all AIS IAVA compliant? (USAREUR Command Policy Letter 4)		
*47. Has the most recent version of the required RCERT-E Baseline been applied to all AIS? (USAREUR Command Policy Letter 4)		

Rating Standard – Information Systems Security:

- Commendable – GO on 40 and above of the questions without missing any critical items listed below.
- Satisfactory – Go on 31-40 of the questions without missing any critical items listed below.
- Needs Improvement – GO on 30 or fewer questions.

∗ These are questions, or similar to questions, that also appear on the Management Control Program (MCP).

Inspector's Comments Mandatory for all NO GO items. (Attach additional sheets if necessary.)

NOTES:

VERIFICATION

X_____
Unit POC's Signature, Name Rank, Date

X_____
Inspector's Signature, Name Rank, Date